UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/086,516	02/28/2002	Khanh V. Nguyen	50325-0644	2155

29989 7590 08/07/2006

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 08/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/086,516	NGUYEN ET AL.	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 May 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13,24,26,28 and 30-53* is/are pending in the application.

4a) Of the above claim(s) *14-23, 25, 27, and 29* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13,24,26,28 and 30-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendments and Arguments

1. Applicant's arguments with respect to amended claims 1, 6, 24, 26, cancelled claims 14-23, 25, 27 and 29, added claims 30-53, and presently pending claims 1-13, 24, 26, 28, and 30-53 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-13, 24, 26, 28, and 30-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hori et al. USPN 6,792,280 B1 in view of J. Franks et al. herein after Franks "An Extension to HTTP: Digest Access Authentication".

Regarding claims 1, 24, and 26, Hori et al. discloses a machine implemented method/medium/apparatus for securing data in communications between a client and server using an unencrypted transfer protocol that does not encrypt a payload defined by the transfer protocol, the method comprising the computer-implemented steps of:

selecting a subset of data for encryption from a set of data to be communicated between the client and the server in a particular payload of the unencrypted transfer protocol (col. 24 lines

11-64, and fig. 18-19 element S115; *downloading server selects ({KPmc(1)}Kpma) to generate unique common key and encrypt session between downloading server and client cell phone in a payload/communication*);

determining a secret integer that is unique (*common key Ks1, Ks2.. unique to each session*) for the subset among a plurality of subsets in a plurality of payloads, wherein the secret integer associated with the particular payload is unique relative to secret integer associated with other payloads of the plurality of payloads (col. 24 lines 38-64; *unique common key is determined and generated for a communication... Ks1, Ks2, ...*);

encrypting the subset of data using at least the secret integer to generate encrypted data that is impractical for a device other than the client and the server to decrypt (col. 24 lines 58-64 and fig. 19 element S113; *encrypting subset of data i.e. (Ks2//KPm(1)) using unique common key Ks1*); and

sending, from a sending device of the client and the server to a receiving device of the client and the server, in the particular payload, the encrypted data (*Ks2*), only at the client and the server, the secret integer for decrypting the encrypted data (col. 25 lines 2-3 and fig. 18. element S139; transmitting).

Hori et al. fails to include a clue information to determine the secrete integer for decrypting the encrypted data.

However Franks discloses a clue information to determine the secrete integer for decrypting the encrypted data. (2.1.1, 2.1.2 and 2.1.3; *nonce, realm, domain,...).*

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Franks within the system of unique common

key generation of a communication. One would have been motivated to do so because the clue information would provide information for generation of decryption secrete key.

Regarding claim 28, it has similar limitations as claim 1, and it has been rejected based on the same rational as claim 1. In addition, Hori et al. discloses the additional limitations of claim 28 wherein:

a network interface that is coupled to the data network for sending one or more packet flows thereto (col. 11 lines 7-24 and fig. 6 element 18);

a processor (fig. 8); and

one or more stored sequences of instructions which, when executed by the processor, causes the processor to carry out the steps of claim 1 limitations (col. 17 lines 52-66).

Regarding claims 2, 30, and 42, Hori et al. and Franks further teach a method, wherein the unencrypted transfer protocol is Hypertext Transfer Protocol (HTTP) (Hori et al. col. 6 lines 28-44, and Franks section 2.1).

Regarding claims 4, 32, and 44, Franks further teaches a method, said step of sending the information to determine the secret integer further comprising the steps of

determining a second public key associated with the sending device based on the first integer (section 2.1.1-2.1.2); and

including the second public key in the information to determine the secret integer (section 2.1.1-2.1.2).

Regarding claims 5, 33, and 45, Franks teaches a method, said step of sending the information to determine the secret integer further comprising the steps of:

determining a plurality of second public keys associated with the sending device based on the first integer, wherein each of the second public keys is associated with one of a plurality of subsets from the set of data (section 2.1.1-2.1.2); and

including the plurality of second public keys in the information to determine the secret integer (section 2.1.1-2.1.2).

Regarding claims 6, 34, and 46, Franks further discloses a method, said step of setting the secret integer further comprising the step of applying a particular hash function to the shared secret key to generate the secret integer (section 2.1.1).

Regarding claims 7, 35, and 47, Franks further teaches a method, said step of generating encrypted data further comprising the step of performing an exclusive or (XOR) operation between corresponding bits of the subset and the secret integer to generate the encrypted data (section 2.1.1; *concatenating data with secrete*).

Regarding claims 8, 36, and 48, Franks further teaches a method as recited, wherein:

said step of determining the secret integer further comprises the step of applying a particular hash function a plurality of times to a shared secret key shared with the receiving device (section 2.1.1); and

said step of sending the information to determine the secret integer further comprises the step of storing, as part of the clue information, data that indicates a number of times the particular hash function has been applied (section 2.1.1; *data string is uniquely generated/hashed each time response/payload is made*).

Regarding claims 9, 37, and 49, Franks further teaches a method, said step of determining the secret integer further comprising the steps of:

determining a first integer formed after the particular hash function is applied the number of times indicated in the information (section 2.1.1);

determining a second integer formed after the particular hash function is applied fewer times than the number of times indicated in the information (section 2.1.1-2.1.2); and

performing an exclusive or (XOR) operation between corresponding bits of the first integer and the second integer (section 2.1.1).

Regarding claims 10, 38, and 50, Franks further teaches a method, said step of determining the secret integer further comprising the steps of

determining a first integer formed after the particular hash function is applied the number of times indicated in the information (section 2.1.1);

determining a second integer formed after a second hash function is applied for the number of times indicated in the information, wherein the second hash function is different from the particular hash function that is used to determine the first integer (section 2.1.1-2.1.2); and

performing an exclusive or (XOR) operation between corresponding bits of the first integer and the second integer (section 2.1.1).

Regarding claims 11, 39, and 51, Franks further teaches a method, further comprising, before said step of determining the secret integer, performing the steps of

determining the shared secret key based on a particular communication between the client and the server (abstract, and section 2.1.1-2.1.2); and

storing the shared secret key in a secure data structure (abstract, and section 2.1.1-2.1.2).

Regarding claims 12, 40, and 52, Franks further teaches a method, wherein the secret integer has a particular number of bits fixed for all subsets in all payloads communicated during a communication session between the client and the server (abstract and page 5 par. 1-7).

Regarding claims 13, 41, and 53, Franks further teaches a method, wherein the secret integer has a number of bits that varies in accordance with lengths of payloads that are communicated during a communication session between the client and the server (page 5 par. 1-7).

Allowable Subject Matter

4. Claim 3, 31, and 43 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claims 1, 26, and 28 respectively and any intervening claims.

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

E. S.
August 2, 2006

NASSER MOAZZAMI
PRIMARY EXAMINER

8/3/06